AFAL-TR-72-113

AD 746029

NINETEEN RULES FOR AVIONICS DESIGN ENGINEERS

Albert Goldman

TECHNICAL REPORT AFAL-TR-72-113

May 1972

Approved for public release; distribution unlimited.

Air Force Avionics Laboratory
Air Force Systems Command
Wright-Patterson Air Force Base, Ohio

UNCLASSIFIED
Security Classification

DOCUMENT CONTROL DATA - R & D

(Security classification of title, body of abstract and indexing annotation must be entered when the overall report is classified)

1. ORIGINATING ACTIVITY (Corporate author) Air Force Avionics Laboratory Wright-Patterson AFB, Ohio 45433	2a. REPORT SECURITY CLASSIFICATION Unclassified 2b. GROUP

3. REPORT TITLE

NINETEEN RULES FOR AVIONICS DESIGN ENGINEERS

4. DESCRIPTIVE NOTES (Type of report and inclusive dates)

5. AUTHOR(S) (First name, middle initial, last name)

Albert Goldman

6. REPORT DATE	7a. TOTAL NO. OF PAGES	7b. NO. OF REFS
May 1972	13	

8a. CONTRACT OR GRANT NO. b. PROJECT NO. c. d.	9a. ORIGINATOR'S REPORT NUMBER(S) AFAL-TR-72-113 9b. OTHER REPORT NO(S) (Any other numbers that may be assigned this report)

10. DISTRIBUTION STATEMENT

Approved for public release; distribution unlimited.

11. SUPPLEMENTARY NOTES	12. SPONSORING MILITARY ACTIVITY
	Air Force Avionics Laboratory Wright-Patterson AFB, Ohio 45433

13. ABSTRACT

Despite the use of integrated circuits, military avionics equipment has increased in cost and complexity, so that acceptable reliability is still a problem. As an aid to designers of avionics subsystems, nineteen rules for assuring reliable products and avoiding possible pitfalls in test and evaluation activities are presented.

DD FORM 1 NOV 65 1473

ia

UNCLASSIFIED
Security Classification

UNCLASSIFIED
Security Classification

14. KEY WORDS	LINK A		LINK B		LINK C	
	ROLE	WT	ROLE	WT	ROLE	WT
Reliability						
Avionics Design						
Avionics Engineering						
Avionics Test and Evaluation						
Avionics Components						

UNCLASSIFIED
Security Classification

AFAL-TR-72-113

NINETEEN RULES FOR AVIONICS DESIGN ENGINEERS

Albert Goldman

iC

FOREWORD

This report was prepared by Mr. Albert Goldman, Staff Engineer in Technical Operations, AFAL/DO. It is based on a paper by Robert Russer, U.S. Army Redstone Arsenal, published 7 Dec 1955; but it has been revised, modernized, and broadened to apply to avionics. It should be useful to younger engineers, and should also be a reminder to experienced engineers.

Submitted by the author 27 March 1972.

This report has been reviewed and is approved.

Warren M. Hansen
WARREN M. HANSEN
Chief, Technical Operations Office

ABSTRACT

Despite the use of integrated circuits, military avionics equipment has increased in cost and complexity, so that acceptable reliability is still a problem. As an aid to designers of avionics subsystems, nineteen rules for assuring reliable products and avoiding possible pitfalls in test and evaluation activities are presented.

NINETEEN RULES
FOR AVIONICS DESIGN ENGINEERS

Despite the use of integrated circuits, military electronic equipment has increased in complexity and cost, so that acceptable reliability and serviceability are still among the top problems of the Defense Department.

The goals of reliability and low cost of ownership demand strict attention to specifications, simplicity in construction, and where practical, testing to failure.

Since the overall reliability of a complex electronic system equals not the average but the product of the reliabilities of its components, if a missile subsystem contains 100 components each having 99% reliability (a widely accepted standard of quality), the overall reliability would turn out to be only 36.5%. In a subsystem with 1000 components having the same 99% reliability, the overall reliability would turn out to be only 0.005%.

The reliability formula indicates, furthermore, that in order to achieve an overall reliability of 80% for a missile containing 4000 components (which is not unusual) one can tolerate, on the average, not more than one failure in 18,000.

As an aid to the designers of avionics subsystems and their components, the following nineteen rules are offered:

1. Reliability is a probability that an item will operate successfully under service conditions. Recognize clearly this mathematical implication; study the basic concepts of statistics and probability.

2. Avoid Rube Goldberg designs. Unreliability goes up with the square of the number of the components. A very complex design may never become reliable and serviceable. Simplicity should be the art, vocation, and objective of every designer.

3. Mistrust the concept of redundancy unless you include foolproof ways to switch to the stand-by components.

4. Mistrust the concept of Environmental Testing. It teaches that missiles and their components can be debugged prior to flight by shaking, shocking, or pre-aging. Actually, bugs may not only be tested out but may also be tested in because some components may become fatigued and fail later.

5. Mistrust flight testing as a means of improving reliability. Since missiles are not usually recoverable, and telemetry and instrumentation are neither perfect nor complete, it is difficult to determine the "ultimate" cause of a failure.

6. Mistrust any specification unless you have determined that it is really applicable to the specific subsystem or component.

7. Get from those responsible for the system design, the actual environmental conditions to be encountered. Replies may be vague, but insist upon an answer. If your subsystem should fail, you are responsible and may have to take the blame for making a guess.

8. If numerical values for environmental conditions have not yet been determined, make a generous estimate and apply safety factors (of about 10); the less the environmental condition is known, the greater should be the safety factor applied to the estimate. Once the condition has become known, say through flight tests, you may find it desirable to reduce the safety factor. This is preferable to having to beef up the components at a later stage, which is costly and strenuously resisted by the system engineers.

9. Never worry that the reliability of your components is too high. Rather, strive for "absolute" reliability; that is, make sure that the probability of failure will be not more than one unit in 10,000 or, better, one in 100,000, under service conditions. Only then may you be sure that your component will never "kill" an expensive missile. Consider every component as a potential "killer" of a missile until you have proof that it is highly reliable. Mistrust any claim of "high quality" and "maximum reliability" unless you know that the selected component can stand the environment with unusually high safety factors.

10. Prove the existence of these high safety factors by testing all component types to failure. This will help you to determine the modes of failure; that is, the predominant weaknesses of the component. By feeding back such knowledge into design, you may raise the reliability of your components considerably, sometimes by orders of magnitude.

11. Do not believe that the test to failure method is intolerably expensive. It may cause additional effort and worry to you and to the test laboratories, but in the long run it will pay high dividends because it is virtually the only way to raise the reliability of your component up to the required "absolute" level and to make your subsystem reliable and serviceable.

12. In planning a test-to-failure program for your component, black box, or subsystem, anticipate all conceivable modes of failure, even if some may appear to be remote. The weapon system may be a million times more expensive than your component.

13. It is not just the environment of shock and vibration that needs to be considered in a test-to-failure program. Many other design criteria may be hazardous, such as maladjustments, misalignments, electrical and mechanical instabilities, structural overloads, friction, insufficient power supplies, and mechanical and electrical resonances. Whenever you have the slightest suspicion that one of these design criteria may become hazardous to your subsystem, insist that it be included in the test-to-failure program. Suspicion is the father of reliability; optimism and gullibility ruin it.

14. Do not rely on test results of just one unit. A subsequent unit might be much weaker. Test a statistically significant number of units.

15. After you have achieved the required "absolute" design reliability of your component, make sure that it is maintained in production and operation. Follow your component through all subsequent phases of production, assembly, inspection, transportation, storage, and operation. You may detect new unexpected weaknesses.

16. See that periodic tests-to-failure, on a sampling basis, are performed as long as your subsystem is being produced.

17. Insist that Statistical Quality Control be applied to your subsystem. However, make sure that proper yardsticks of reliability are applied. Typically, not more than 1 out of 10,000 units should be permitted to fail.

18. Should your component show a weakness, confer with the manufacturer. The failure might have originated in your own design oversight.

19. Keep in close contact with users. Your subsystem may have high intrinsic reliability, yet it may be useless if this reliability cannot be maintained in service.